Compliance Component

DEFINITION	
Name	Securing Remote Computers and Connections
Description	Securing Remote Computers and Connections is ensuring the confidentiality, integrity and availability of information transmitted via a public provider. Remote access includes, but is not limited to: • DSL • Cable • Wireless • Satellite • ISDN • Broadband over Power Line (BPL)/Power Line Communications (PLC) • Dial-up
Rationale	Remote Computers can pose a higher risk if improperly configured. In addition, broadband connections are always connected, which pose an even higher risk for security compromise. Due to the growth in the number of telecommuters and other remote users, there is an increasing number of people who need secure remote access.
Benefits	• Provides a means of securing a system that is connected to an agency via a public provider
ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Remote Access Controls
List Product Component Name	
COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	
COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	<u>Securing Remote Computers</u> • Only agency-approved equipment may be remotely connected to the agency network • Virus protection software must be installed and kept current on remote systems

	• A firewall must be installed and properly configured on all remotely connected systems (see the Firewall Rules Compliance Component)
	• Computers connected to the agency network shall not simultaneously connect to any other network via another network device, i.e., internal modem, external modem, Network Interface Card (NIC), wireless NIC, etc.
	  o Split-tunneling must not be enabled on the VPN
	  o Shares between the agency computer and non-agency systems must be disabled when the remote computer is connected to the agency network
	• Operating systems must be kept up-to-date on remote computers per agency requirements
	• Remote computers must be disconnected from the network when not in use
	• Critical data must be moved from the local drive of a remote computer to an agency server as soon as feasible
	
	<u>Securing Remote Connections</u>
	• Agency approval is required before any user may connect remotely to the agency network
	• Remote connections must meet the cryptography compliance component requirements (see Cryptography for VPN and Cryptography for Web Servers)
	• Remote connections used for transmitting CONFIDENTIAL information must meet the Advanced/Strong Authentication compliance component

Document Source Reference #	NIST Special Publication 800-46, Security for Telecommuting and Broadband Communications
Standard Organization	
Name	NIST, CERT®Coordination Center — *Website*: csrc.nist.gov, www.cert.org
Contact Information	
Government Body	
Name	*Website*
Contact Information	
KEYWORDS	
List all Keywords	Broadband, Cable, Digital Subscriber Line (DSL), Wireless, Broadband over Power Line (BPL), Power Line Communications (PLC), Satellite, Modem, Internet, Virtual Private Network (VPN), Dial-Up, Network Interface Card (NIC)
COMPONENT CLASSIFICATION	
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*
Rationale for Component Classification	
Document the Rationale for Component Classification	

Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	03/31/2005	*Date Accepted / Rejected*	11/08/05
Reason for Rejection			
Last Date Reviewed	09/29/2005	*Last Date Updated*	09/29/2005
Reason for Update	Clarified for simultaneous network connections		